State of West Virginia Office of Technology
Policy: Anti-Virus
Issued by the CTO

1.0 PURPOSE

The purpose of anti-virus software is to provide Executive Branch agencies with comprehensive protection against computer viruses and other malicious computer code also known as “malware”. This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, desktops, workstations, and laptops/notebooks, which are either physically or remotely connected to the State network via a standard network, wireless, modem, or through virtual private network (VPN).

This policy describes the measures taken by the West Virginia Office of Technology (WVOT) to counter computer viruses and identifies the responsibilities of the WVOT, as well as all Executive Branch employees, in protecting the State network against viruses.

2.0 SCOPE

This procedure applies to all Executive Branch employees and all equipment attached to WVOT networks.

3.0 RELEVANT DOCUMENTS/MATERIAL

3.1 West Virginia Office of Technology (WVOT) Web Page

3.2 WVOT Web Site Home Page - IT Security Web Policies Issued by the Chief Technology Officer (CTO).

3.3 West Virginia Code §5A-6-4a Controls – “Duties of the Chief Technology Officer Relating to Security of Government Information”

3.4 WVOT-PR1016 – Virus Reporting

3.4 WVOT-PO1001 – Information Security Policy and Appendix A

3.5 WVOT-PO1004 – Acceptable Use of Portable Devices

3.6 WVOT-PR1005 – E-mail Guidelines

4.0 POLICY

4.1 WVOT will evaluate, procure, install, and maintain anti-virus software and/or tools for use on all WVOT supported desktop computers, laptops, servers, and other computing devices.

4.2 All software **must** be installed by WVOT technicians.

4.3 All workstations and servers connected to Executive Branch computer network resources must have WVOT-managed anti-virus software installed, configured, and activated.

4.4 Data and program files that have been electronically transmitted to a WVOT supported computer from another location, whether internal or external, will be automatically scanned for viruses.

4.5 The WVOT will ensure that all remote workstations and servers used by State employees, contractors, and third-party contractors and/or providers accessing internal networks are protected with virus-scanning software equivalent to that used by the State for network-attached devices.

4.6 The WVOT will configure systems to prevent users from disabling anti-virus software updates and virus scans.

4.7 Anti-Virus Coordinator Responsibilities (see WVOT-PR1016, *Virus Reporting*)

4.7.1 The WVOT Anti-Virus Coordinator will monitor supported networks for virus incidents and ensure that a reliable process is in place to receive and distribute updated virus definitions from anti-virus software vendors to protect against new virus threats.

4.7.2 The Anti-Virus Coordinator will respond to alerts of virus incidents and advise the WVOT Client Services Management of any special procedures or precautions required for common or prevalent viruses.

5.0 STANDARD PRACTICES

5.1 The Anti-Virus Team Lead will retain anti-virus log files for a period of time designated by the WVOT. A report will be presented monthly to the Chief Information Security Officer (CISO).

5.2 The Anti-Virus Team Lead must create and ensure the implementation of to the CISO on a monthly basis. Reports should include virus statistics broken down by type.

5.3 Employee Responsibilities (see WVOT-PR1016)

5.3.1 Employees will only use software provided by the State.

5.3.2 Employees must not intentionally introduce a virus onto State computing equipment or systems, or withhold information necessary for effective virus control procedures.

5.3.3 Employees should use extreme caution when executing programs or opening e-mail attachments that: (1) have not been requested; or (2) come from an unknown source.

5.3.4 Employees must not attempt to alter or disable anti-virus software, or attempt to terminate any scan being performed by anti-virus software, on any system attached to the Executive network.

6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing agency and may be based on recommendations of the WVOT and the West Virginia Division of Personnel, intended to address severity of the violation and the consistency of sanctions.

7.0 LEGAL AUTHORITY

Under the provisions of West Virginia Code §5A-6-4a *et seq*., the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

8.0 DEFINITIONS

8.1 Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within Executive Branch agencies.

8.2 Anti-Virus Software – Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.

8.3 Anti-Virus Team Lead – The functional supervisor of the Anti-Virus Team.

8.4 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

8.5 Chief Technology Officer (CTO) - The person responsible for the State's information resources.

8.6 Computer Virus – A piece of potentially malicious software that is designed to cause some unexpected or undesirable event, and is

generally introduced to a system without the knowledge or consent of the user.

8.7 Contractor – Anyone who has a contract with the State or one of its entities.

8.8 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

8.9 Office of Information Security and Controls (OISC) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a.

8.10 Scan – To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors, et. al.).

8.11 West Virginia Division of Personnel – The Division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.,* which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

8.12 West Virginia Office of Technology (WVOT)- The division of the Department of Administration established by West Virginia Code §5A-6-4a, *et. seq*., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

8.13 Workstation – A personal computer; also called a PC.

9.0 INDEX

R

S

V

W